

## **SECMAN OPTIONS**

(This page has been intentionally left blank.)

## CHAPTER 7: SECMAN INTRODUCTION

Unified Build (UB) is an automated Command, Control, Communications, Computers, and Intelligence (C<sup>4</sup>I) application, which interfaces to a variety of military communications and computer systems. Chapter One of the *Unified Build User's Guide* contains more complete information about UB.

The SECMAN portion of this guide provides information about UB security administration in the GENSER and SCI environments. The Security Manager, or a user assigned a Security Admin role, performs basic tasks such as maintaining user accounts and audit logs.

The following chapters describe menus and options available on the menu bar of the SECMAN login.

### SYSTEM MENU

Options to set menu font size for the security application and to exit the system. .... 87

### SECURITY MENU

Options to update audit status, review audit information and archive audit logs. .... 91

### ACCOUNTS MENU

Options to create, edit, review, maintain, archive, restore, and export roles and user accounts. .... 101

### PRINTING

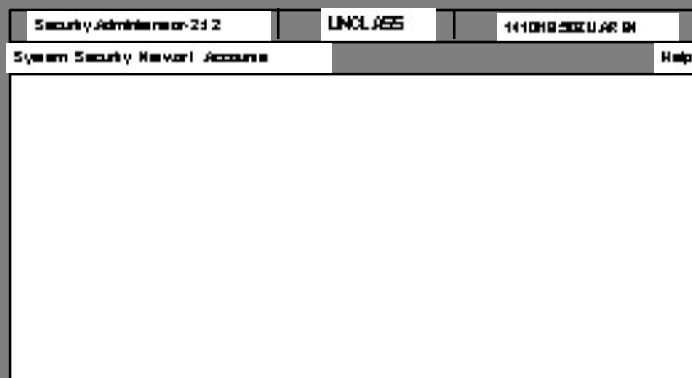


Figure 7-1 Security Application Menu Screen

## **Notes**

## CHAPTER 8: SYSTEM MENU

The System menu contains options to change the window and menu font size or to exit from the security application.

### 8.1 SET WINDOW FONT

Use this option to set the font size for windows in the security application, including the pop-up menus.

- Windows and pop-up menus will be sized in proportion to the font size.
- When the font is changed, the change does not take effect until a new window is opened.
- The new font is saved as the default and will continue to be used, even when the system is shut down and restarted.

**To access this window:** SYSTEM menu : SET WINDOW FONT option : SELECT A WINDOW FONT window.

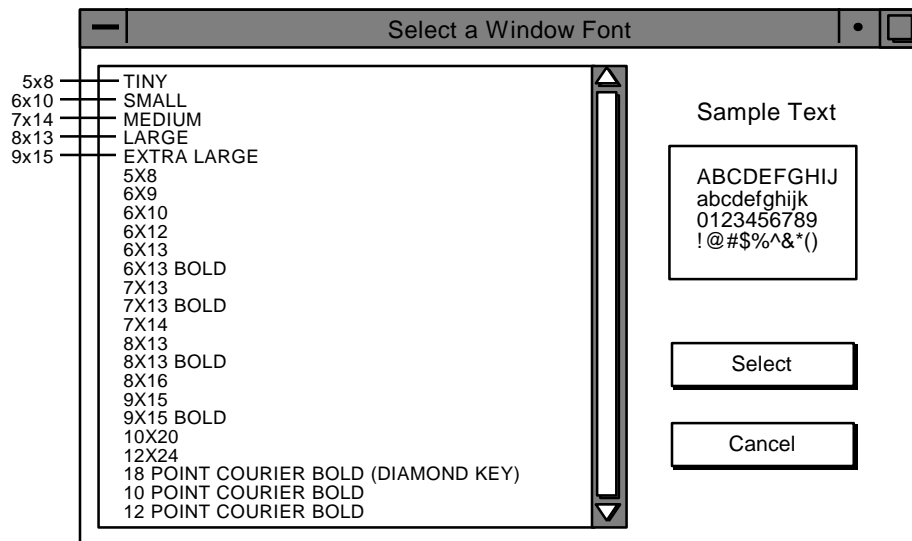


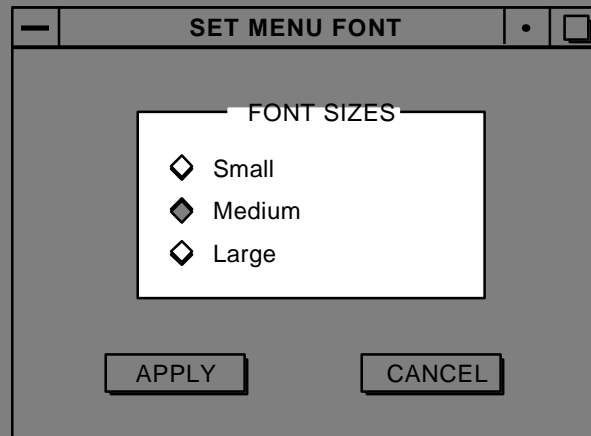
Figure 8-1 Select a Window Font

1. Highlight any font on the list. When a font is highlighted, its characters are shown in the SAMPLE TEXT box.
2. Click SELECT to change the font (or CANCEL to discard the change). When the font is changed, the change *does not* take effect until a new window is opened.

## 8.2 SET MENU FONT

Use the SET MENU FONT option to set the font size for the menus within the security application.

**Access this window:** SYSTEM menu : SET MENU FONT option : SET MENU FONT window (Figure 8-2).



*Figure 8-2 Set Menu Font*

1. Select SMALL, MEDIUM, or LARGE diamond knob.
2. Click APPLY to accept the change and close the window.
3. Click CANCEL to discard any changes made since the last APPLY and close the window.
4. Choose SYSTEM EXIT from the SYSTEM menu and restart the security application for the change to take effect.

Pop-up menu options, APPLY and CANCEL, function the same as the window buttons.

## 8.3 SYSTEM EXIT

The System Exit option closes all windows and returns the user to the login prompt.

**Notes**

## **Notes**



## CHAPTER 9: SECURITY MENU

The Security menu contains options to maintain audit status and audit logs on the workstation. Log on to each workstation operating on the LAN to set its audit status.

### 9.1 AUDIT STATUS

Use this option to:

- Designate SECURITY, AUDITING, or both, as ON or OFF.
- Set level of granularity, the *level of detail*, for information that should be logged on the workstation.
- View current log sizes to determine when logs should be archived or purged.

**To access this window:** SECURITY menu : AUDIT STATUS option : AUDIT STATUS window (Figure 9-1).

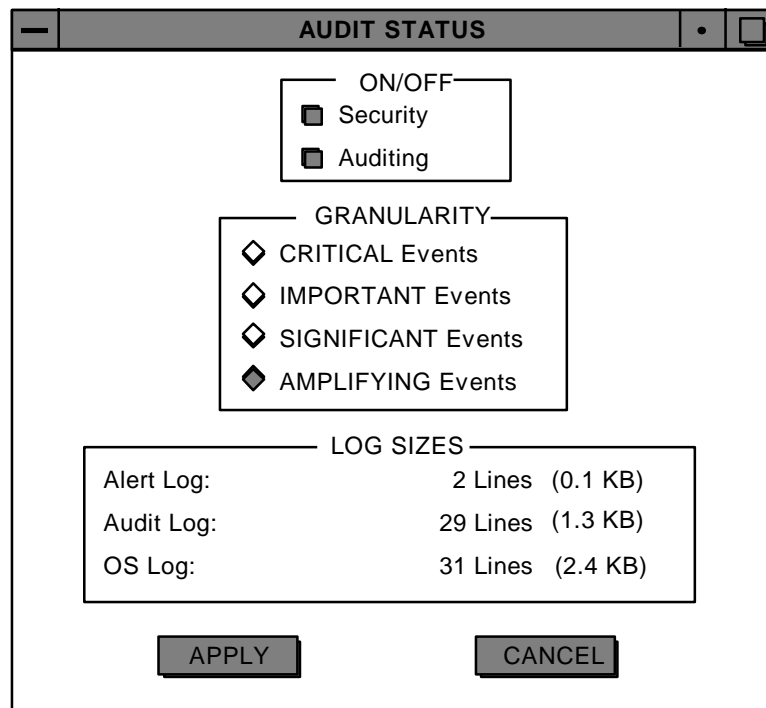


Figure 9-1 Audit Status

***How to use the AUDIT STATUS window:***

1. Toggle SECURITY and AUDITING fields ON or OFF.
2. Click the appropriate diamond knob to select the level of granularity.
3. Click APPLY to accept the changes or CANCEL to discard them. Clicking either button closes the window.

Pop-up menu options, APPLY and CANCEL, function the same as the window buttons.

**9.1.1 ON/OFF BOX**

Each application running on the workstation determines which events from that application will be logged. An application can assign one or more of the following commands to an event:

- |                     |   |
|---------------------|---|
| <b>Audit Event</b>  | An entry is written in the SECURITY AUDIT LOG if AUDITING is toggled ON and the granularity level is sufficiently detailed. (AUDITING cannot be toggled ON unless SECURITY is also toggled ON.) |
| <b>Always Audit</b> | An entry is written in the SECURITY AUDIT LOG regardless of the AUDIT STATUS settings.  |
| <b>Alert Event</b>  | An entry is written in the SECURITY ALERT LOG if SECURITY is toggled ON.  |

When an event is assigned both an audit command and an alert command:

- The event will be written in both logs if SECURITY and AUDITING are toggled ON.
- The event will be written only in the SECURITY ALERT LOG if SECURITY is toggled ON and AUDITING is toggled OFF.

The following CRITICAL events within the security application are assigned the Always Audit command and will always be entered in one or both logs:

- Auditing Enabled (AUDITING toggled ON.)
- Auditing Disabled (AUDITING toggled OFF.)
- Global Security Enabled (SECURITY toggled ON.)
- Global Security Disabled (SECURITY toggled OFF.)

### **9.1.2 GRANULARITY BOX**

The following granularity levels form a hierarchy; “Critical” auditing provides the least amount of information, while “Amplifying” provides the most.

#### **CRITICAL Events**

Logging in and out; updating, exporting, or archiving user accounts or roles; archiving and purging logs; changing the audit status; and changing the security classification.

#### **IMPORTANT Events**

All CRITICAL Events *plus* user entry or exit of classified functions.

#### **SIGNIFICANT Events**

All IMPORTANT Events (and, therefore, all CRITICAL Events) *plus* printing or archiving data.

#### **AMPLIFYING Events**

All of the above *plus* all information applications installed on the workstation are designed to collect, such as modifying data in window fields.

### **9.1.3 LOG SIZES BOX**

The size of each log is indicated in number of lines (each line representing one event) and in kilobytes. Log sizes are updated as audit records are added. Use the information in this box to determine when logs should be archived and purged.

## **9.2 AUDIT LOG**

Each workstation operating on the LAN generates an Audit Log. Each log lists audit events generated by applications running on that machine. Events listed have occurred since the log was last purged.

Events will be logged only if SECURITY and AUDITING are toggled ON in the AUDIT STATUS window.

Because applications determine which events are logged, a comprehensive list of entries for this window is not possible.

**To access this window:** SECURITY menu : AUDIT LOG option : SECURITY AUDIT LOG window (Figure 9-2).

SECURITY AUDIT LOG					
DTG	W/S	USER	GRAN LEVEL	APP	AUDIT EVENT
131435:04Z Mar 94	gccs3	SSO	CRITICAL	SSO	Logged In
131434:59Z Mar 94	gccs3	root	CRITICAL	SSO	Logged Out
131434:04Z Mar 94	gccs3	root	CRITICAL	SSO	Logged In
131433:37Z Mar 94	gccs3	ntcs	CRITICAL	SSO	Logged Out
101715:15Z Mar 94	gccs3	ntcs	CRITICAL	SSO	Logged In
101715:09Z Mar 94	gccs3	secman	CRITICAL	SSO	Logged Out
101713:16Z Mar 94	gccs3	secman	CRITICAL	SSO	Logged In
101713:07Z Mar 94	gccs3	jotsii	CRITICAL	SSO	Logged Out
101711:30Z Mar 94	gccs3	jotsii	CRITICAL	SSO	Logged In
101711:14Z Mar 94	gccs3	secman	CRITICAL	SSO	Logged Out
101710:37Z Mar 94	gccs3	secman	CRITICAL	SSO	Logged In
101642:53Z Mar 94	gccs3	halt	CRITICAL	SSO	Logged In

PRINT
ARCHIVE
PURGE
EXIT

Figure 9-2 Security Audit Log

Click on a column heading to sort the list by that heading. The default sort is the date-time group, listing the most recent record first.

#### **SECURITY AUDIT LOG Window Buttons:**

PRINT– generates a printed report of the window contents. (Described in *Printing*.)

ARCHIVE– saves window information to tape. (Described in *Archive Logs*.)

PURGE– removes all audit information from the log. NOTE: Archiving a log before purging is strongly recommended.

EXIT– closes the window.

#### **SECURITY AUDIT LOG Pop-up Menu Options**

Pop-up menu options, PRINT, ARCHIVE, PURGE and EXIT, function the same as the window buttons.

#### **SECURITY AUDIT LOG Window Fields:**

Each audit entry contains:

##### **DTG**

Date-time group when the audit event occurred.

**WORKSTATION**

The name of the workstation where the audit event occurred.

**USER**

User at the time of the audit event.

**GRAN LEVEL**

Granularity of the audit event. (Described in *Audit Status*.)

**APPLICATION**

Application that generated the audit event.

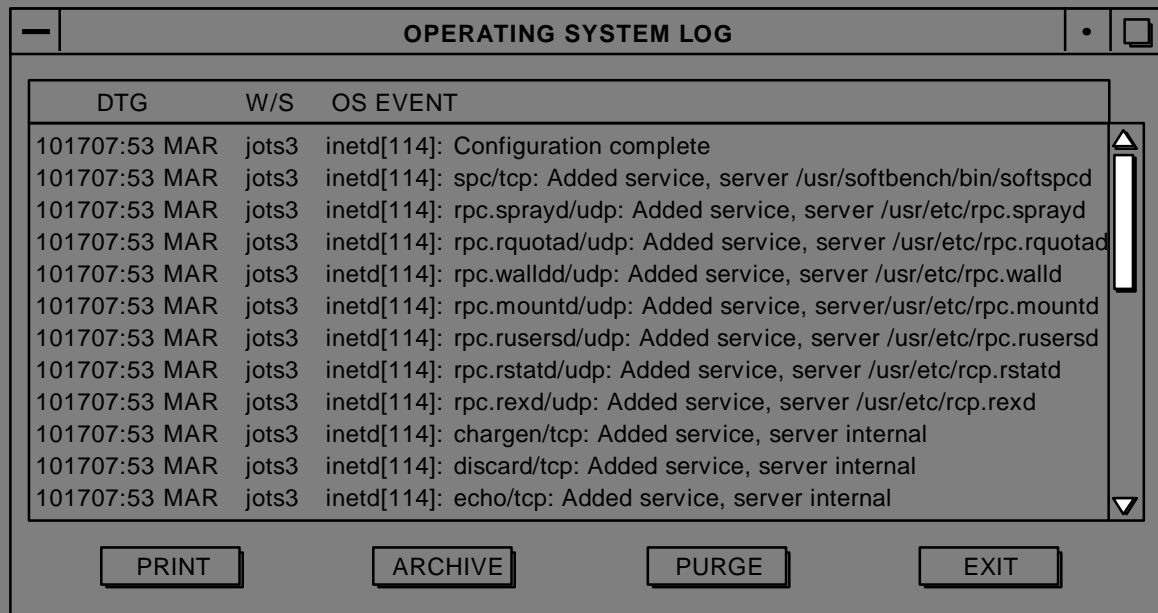
**AUDIT EVENT**

Description of the audit event.

### 9.3 OS AUDIT LOG

Each workstation operating on the LAN generates an Operating System (OS) Log. This log lists events generated by the operating system on that machine. Events listed have occurred since the log was last purged.

**To access this window:** SECURITY menu : OS AUDIT LOG option : OPERATING SYSTEM LOG window (Figure 9-3).



DTG	W/S	OS EVENT
101707:53 MAR	jots3	inetd[114]: Configuration complete
101707:53 MAR	jots3	inetd[114]: spc/tcp: Added service, server /usr/softbench/bin/softspcd
101707:53 MAR	jots3	inetd[114]: rpc.sprayd/udp: Added service, server /usr/etc/rpc.sprayd
101707:53 MAR	jots3	inetd[114]: rpc.rquotad/udp: Added service, server /usr/etc/rpc.rquotad
101707:53 MAR	jots3	inetd[114]: rpc.walldd/udp: Added service, server /usr/etc/rpc.walldd
101707:53 MAR	jots3	inetd[114]: rpc.mountd/udp: Added service, server /usr/etc/rpc.mountd
101707:53 MAR	jots3	inetd[114]: rpc.rusersd/udp: Added service, server /usr/etc/rpc.rusersd
101707:53 MAR	jots3	inetd[114]: rpc.rstatd/udp: Added service, server /usr/etc/rpc.rstatd
101707:53 MAR	jots3	inetd[114]: rpc.rexd/udp: Added service, server /usr/etc/rpc.rexd
101707:53 MAR	jots3	inetd[114]: chargen/tcp: Added service, server internal
101707:53 MAR	jots3	inetd[114]: discard/tcp: Added service, server internal
101707:53 MAR	jots3	inetd[114]: echo/tcp: Added service, server internal

PRINT ARCHIVE PURGE EXIT

Figure 9-3 Operating System Log

Click on a column heading to sort the list by that heading. The default sort is the date-time group, listing the most recent record first.

***OPERATING SYSTEM LOG Window Buttons:***

PRINT– generates a printed report of the window contents. (Described in *Printing*.)

ARCHIVE– saves window information to tape. (Described in *Archive Logs*.)

PURGE– removes all audit information from the log. NOTE: Archiving a log before purging is strongly recommended.

EXIT– closes the window.

***OPERATING SYSTEM LOG Pop-up Menu Options***

Pop-up menu options, PRINT, ARCHIVE, PURGE and EXIT, function the same as the window buttons.

***OPERATING SYSTEM LOG Window Fields:***

Each OS audit entry contains:

**DTG**

Date-time group when the audit event occurred.

**WORKSTATION**

The name of the workstation where the audit event occurred.

**OS EVENT**

Description of the audit event.

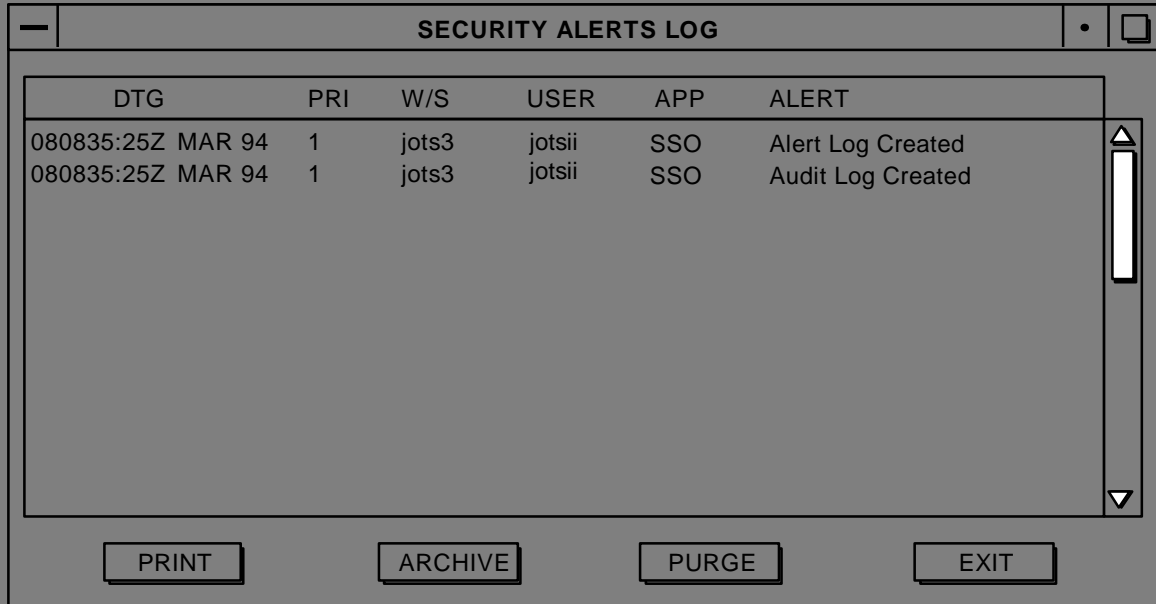
**9.4 SECURITY ALERT LOG**

Each workstation operating on the LAN generates a Security Alerts Log. This log lists events that should be seen by the Security Manager, generated by security applications running on that machine. Events listed have occurred since the log was last purged.

Events will be logged only if SECURITY is toggled ON in the AUDIT STATUS window.

Because applications determine which events are logged, a comprehensive list of entries for this window is not possible.

**To access this window:** SECURITY menu : OS AUDIT LOG option : OPERATING SYSTEM LOG window (Figure 9-4).



DTG	PRI	W/S	USER	APP	ALERT
080835:25Z MAR 94	1	jots3	jotsii	SSO	Alert Log Created
080835:25Z MAR 94	1	jots3	jotsii	SSO	Audit Log Created

*Figure 9-4 Security Alerts Log*

Click on a column heading to sort the list by that heading. The default sort is the date-time group, listing the most recent record first.

***SECURITY ALERTS LOG Window Buttons:***

PRINT– generates a printed report of the window contents. (Described in *Printing*.)

ARCHIVE– saves window information to tape. (Described in *Archive Logs*.)

PURGE– removes all audit information from the log. NOTE: Archiving a log before purging is strongly recommended.

EXIT– closes the window.

***SECURITY ALERTS LOG Pop-up Menu Options***

Pop-up menu options, PRINT, ARCHIVE, PURGE and EXIT, function the same as the window buttons.

**SECURITY ALERTS LOG Window Fields:**

Each audit entry contains:

**DTG**

Date-time group when the audit event occurred.

**PRIORITY**

Priority of the alert.

**WORKSTATION**

The name of the workstation where the audit event occurred.

**USER**

User at the time of the audit event.

**APPLICATION**

Application that generated the audit event.

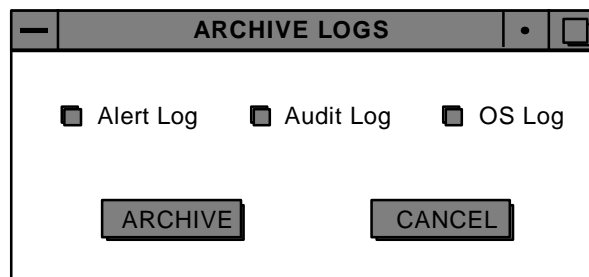
**AUDIT EVENT**

Description of the audit event.

## 9.5 ARCHIVE LOGS

Use this option to save the Alert, Audit, and OS logs to tape.

**To access this window:** SECURITY menu : ARCHIVE LOGS option : ARCHIVE LOGS window (Figure 9-5).



*Figure 9-5 Archive Logs*

**How to use this option:**

1. Toggle ON any combination of logs to be archived.
2. Insert a tape and click ARCHIVE (or, click CANCEL to discontinue the archive process and close the window).



3. Click OK in the confirmation window to verify the archive tape is ready for writing.
4. A second confirmation window appears before proceeding with the archive process.
  - Note: The archive process cannot be canceled after YES is selected.
  - Click YES to continue with the archive, or NO to cancel the process.

Pop-up menu options, ARCHIVE and CANCEL, function the same as the window buttons.

## **Notes**

## CHAPTER 10: ACCOUNTS MENU

The ACCOUNTS menu contains options to create and maintain roles and user accounts. The following topics are covered:

- ROLES
- EXPORT

### USER ACCOUNTS QUICK REFERENCE

Account Group	Login Name	Password	Role Requirement	Role Name	Menu/Option Access	Security Level
root <sup>1</sup>	root <sup>1</sup>	vinson <sup>2</sup>	Not Allowed	N/A	All UNIX Files	N/A
	Assigned by Sec Mgr <sup>3</sup> (see note)	Assigned by Sec Mgr	Not Allowed	N/A	All Unix Files	N/A
Security Admin <sup>1</sup>	secman <sup>1</sup>	vinson <sup>2</sup>	Required	SSO Default <sup>1</sup>	All Security Menus and Options	Secret
	Assigned by Sec Mgr <sup>3</sup>	Assigned by Sec Mgr	Required	Assigned by Sec Mgr	Assigned by Sec Mgr	Assigned by Sec Mgr
System Admin <sup>1</sup>	sysadmin <sup>1</sup>	vinson <sup>2</sup>	Required	SA Default <sup>1</sup>	All System Admin Menus and Options	Secret
	Assigned by Sec Mgr <sup>3</sup>	Assigned by Sec Mgr	Required	Assigned by Sec Mgr	Assigned by Sec Mgr	Assigned by Sec Mgr
GCCS Operator <sup>1</sup>	Assigned by Sec Mgr <sup>3</sup>	Assigned by Sec Mgr	Required	GCCS Default <sup>1</sup>	Basic GCCS Menus and Options (Tracks are view-only)	Secret
	Assigned by Sec Mgr <sup>3</sup>	Assigned by Sec Mgr	Required	Assigned by Sec Mgr	Assigned by Sec Mgr	Assigned by Sec Mgr

Figure 10-1 User Accounts Quick Reference

#### Legend

<sup>1</sup>Preset, cannot edit.

<sup>2</sup>Preset, please change.

<sup>3</sup>A login name (user account) may have multiple account groups and roles assigned.

Note: The root account group allows unrestricted access to all UNIX files. User accounts added to the root account group will have the same unrestricted access.

## 10.1 VIEW ROLES

A role is assigned to each user account that defines a user's classification and access to functions within the menus and options of the assigned account group. Users can perform only those functions defined for their assigned roles.

Applications available with a role, such as Security Administration or System Administration, are specified by the account group selected for the role. The majority of users will be assigned the GCCS Operator account group.

Use this option to:

- create and edit roles with restricted access to menus and options.
- view and maintain a list of roles in the system. The list includes:
  - default roles
  - roles added by the Security Manager (or by any user assigned a security Admin role with permission to add roles).

Three default roles delivered with the system provide access to all functions of the assigned account group:

- SSO Default
  - Security Admin account group
  - Access to all security application menus and options
  - Secret classification
- SA Default
  - System Admin account group
  - Access to all system administration menus and options
  - Secret classification
- GCCS Default
  - GCCS Operator account group
  - Access to all GCCS COE segment and GCCS application segment menus and options

- Secret classification
- Not restricted from editing tracks
- Restricted from modifying ELINT configuration

Note: If selected users require restriction on track management or on ELINT configuration permissions, you must create a new role with Track View restriction and/or without ELINT configuration edit permission. Assign such users to this new role using the Security icon.

Roles can be created which define restricted access to menus and options within the account group. For example, to create an unclassified account for a GCCS Operator that excludes access to the COMMS menu:

1. Create a role within the GCCS Operator account group with COMMS options toggled OFF.
2. Create a new user and assign it to this role.
3. The COMMS menu options will not appear on the main menu bar when that user logs in.

*GCCS Operator*, *System Admin*, and *Security Admin* account groups may have roles associated with them. Roles cannot be created for the *root* account group.

**To access this window:** ACCOUNTS menu : VIEW ROLES option : USER ROLES window (Figure 10-2).

USER ROLES		
ROLE	ACCT GROUP	CLASSIFICATION
GCCSDefault	GCCSOperator	SECRET
SA Default	System Admin	SECRET
SSO Default	Security Admin	SECRET

ADD	DELETE	EDIT	DUPLICATE	PRINT	EXIT
-----	--------	------	-----------	-------	------

Figure 10-2 User Roles

#### **USER ROLES Window Buttons:**

ADD— a role. Described in *Add Role*.

DELETE– a role.

Default roles and roles assigned to a user account cannot be deleted.

1. Highlight one or more roles.
2. Click DELETE. A confirmation window appears to verify the delete.
3. Click YES to confirm the delete (or click NO to cancel). The role is deleted from the USER ROLES list and will not appear in the ROLES list in the ADD ACCOUNT window.

EDIT– a role. Described in *Edit Role*.

DUPLICATE– creates a new role similar to an existing role.

1. Highlight a role.
2. Click DUPLICATE.
3. Type a new role name in the DUPLICATE ROLE window.
4. Click OK to accept the name and close the window (or click CANCEL to discard the role). The duplicate role is listed in the USER ROLES window. Use EDIT to make changes to the new role (described in *Edit Role*).

PRINT– generates a printed report of the window contents (described in *Printing*).

EXIT– closes the window.

### ***USER ROLES Window Fields:***

Each entry in the USER ROLES window includes:

#### **ROLE**

Name of the role.

#### **ACCT GROUP**

Account group associated with the role.

#### **CLASSIFICATION**

Security classification level of the role.

### **10.1.1 ADD ROLE**

Use this option to create a role with restricted access to menus and options within an application.

Click ADD in the USER ROLES window to open the ADD ROLE window (Figure 10-3).

ADD in the USER ROLES window to open the ADD ROLE window (10-3).

The screenshot shows a window titled "ADD ROLE". It contains three main input areas: a text box for "NAME", a dropdown menu for "SECURITY" with "UNCLASS" selected, and a list box for "ACCOUNT GROUPS" with three items: "Security Admin", "System Admin", and "GCCS Operator". At the bottom of the window are two buttons: "OK" and "CANCEL".

Figure 10-3 Add Role

***How to use this option:***

1. Type a role name, not to exceed 15 characters.
2. Type a security classification or its abbreviation
  - Unclassified (U)
  - Confidential (C)
  - Secret (S)
3. Select one account group to determine which application will be available to a user assigned this role.
4. Click OK to accept the new role (or CANCEL to discard).
5. The EDIT ROLE window opens to define the role (described in *Edit Role*).

### **10.1.2 EDIT ROLE**

Edit a role to define access to menus and functions for a new role or to modify an existing role.

- Access to menus and functions can be expanded or reduced.
- When new segments are loaded, additional menus and options will be available. A role can be expanded to include the added functionality.



- When segments are removed, menus and options are automatically deleted from associated roles. However, user accounts assigned the roles will retain the previous role information.
  - Open the EDIT window for each user account and modify at least one field.
  - The user account will then incorporate the revised role. (See EDIT in *View User Accounts*.)

To edit a role, highlight one role in the USER ROLES window (Figure 10-2). Click EDIT to open the EDIT ROLE window (Figure 10-4).

**EDIT ROLE**

**ROLE HEADER**

NAME: secman  
ACCT GROUP: Security Admin  
SECURITY: TOP SECRET

**PERMISSIONS**

Accounts  
Audit Status  
Classification  
Logs  
Roles

A:Add D:Delete E:Edit  
P:Print R:Restore V:Archive  
X:Export

EDIT

**MENU ACCESS**

Sec Admin

EDIT

OK CANCEL

Figure 10-4 Edit Role

**How to use the EDIT ROLES window:**

1. Select a security classification in the ROLE HEADER box.

2. Select functions which will be available in the role in the PERMISSIONS box (described in *Permissions Box*).
3. Select menus and options which will be available for the role in the MENU ACCESS box (described in *Menu Access Box*).
4. Click OK to accept the role, or CANCEL to discard.

#### 10.1.2.1 ROLE HEADER Box

The NAME and ACCT GROUP fields cannot be edited. Only the SECURITY field can be modified.

##### NAME

Name of the role.

##### ACCT GROUP

Account group selected for the role.

##### SECURITY

The classification assigned to the role.

#### 10.1.2.2 PERMISSIONS Box

Use the PERMISSIONS box (Figure 10-5) to define functions available to a user in the role.

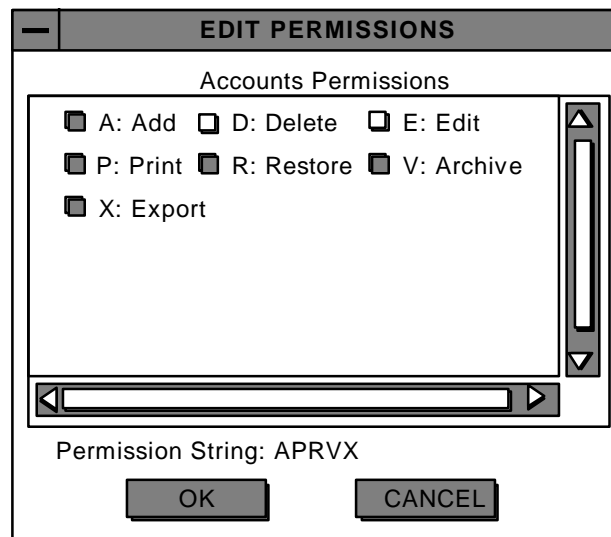
PERMISSIONS	
Category 1	ADE
Category 2	ADEPVRX
<other appropriate categories>	
A:Add	D:Delete E:Edit
<all potential functions>	
EDIT	

Figure 10-5 Permissions Box

Categories and functions will vary with each account group. Functions toggled ON appear as part of the category entry in the scroll list.

**How to use this option:**

1. Highlight one category in the scroll list.
2. Click EDIT to open the EDIT PERMISSIONS window (Figure 10-6).
3. Toggle checkboxes ON for functions to be available to a user assigned this role. (All functions are OFF when a new role is created.)
  - For example, in Figure 10-6 a user could add, print, restore, archive and export, but could not delete or edit.
  - The list of functions shown for the selected category is an appropriate subset of the potential functions.
4. Click OK to accept the changes, or CANCEL to discard. Clicking either closes the window.
5. Repeat steps 1–4 for each category.

*Figure 10-6 Edit Permissions Window***Categories and Available Functions**

Categories and functions are dependent on the account group selected for the role. Each account group with its categories and subset of functions is shown below:

**Security Admin Account Group**

<i>Category</i>	<b>Add</b>	<b>Delete</b>	<b>Edit</b>	<b>Print</b>	<b>Restore</b>	<b>Archive</b>	<b>Export</b>
Accounts	X	X	X	X	X	X	X
Audit Status			X				

# Accounts Menu

Classification			X				
Logs		X		X		X	
Roles	X	X	X	X	X	X	X

**GCCS Operator Account Group**

<b>Category</b>	<b>View</b>	<b>Edit</b>
Tracks	X	
ELINT Config		X

- To restrict TRACKS to view only, toggle the VIEW checkbox ON in the EDIT PERMISSIONS window.
- The GCCS Elint Configuration window is view only. To allow a user to edit the fields in this window, toggle the EDIT checkbox ON in the EDIT PERMISSIONS window.
- All other functions, add, edit, delete, print, restore, and archive, are available and do not appear in the PERMISSIONS box.

**System Admin Account Group**

The System Admin group does not display a PERMISSIONS box.

**root Account Group**

No roles can be created for this account group.

***EDIT PERMISSIONS Pop-up Options:***

Pop-up options OK and CANCEL function the same as the window buttons. The menu also includes:

*SELECT ALL*

Toggles all options ON.

*UNSELECT ALL*

Toggles all options OFF.

**10.1.2.3 MENU ACCESS Box**

The MENU ACCESS box (Figure 10-7) contains a scroll list of the menubars found in the application accessible to a role. Use EDIT to define which menus and options will be available.

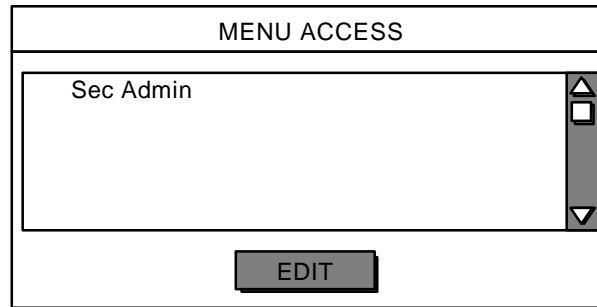


Figure 10-7 Edit Menu Access Window for Security Admin

Click one menubar in the scroll list and click EDIT to open the EDIT MENU ACCESS window (Figure 10-8).

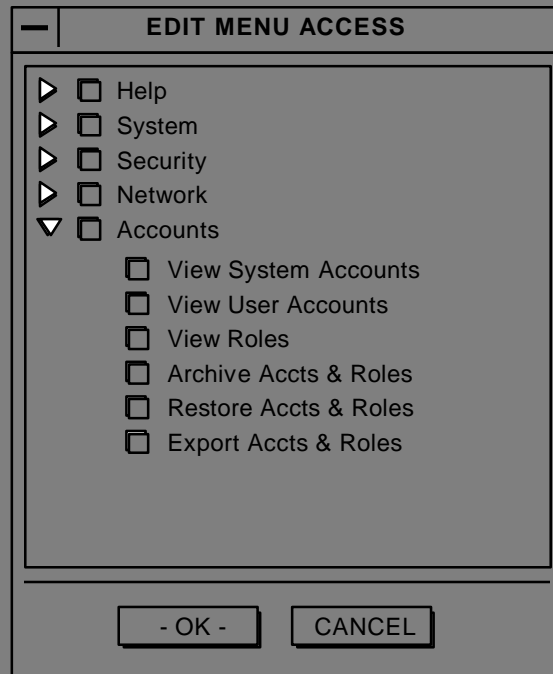


Figure 10-8 Edit Menu Access Window

This window contains a list of menus on the menubar of an application. (Applications are designated by the account group selected for the role.) Click the arrow left of the menu name to reveal a cascading list of options for that menu.

***How to use the EDIT MENU ACCESS window:***

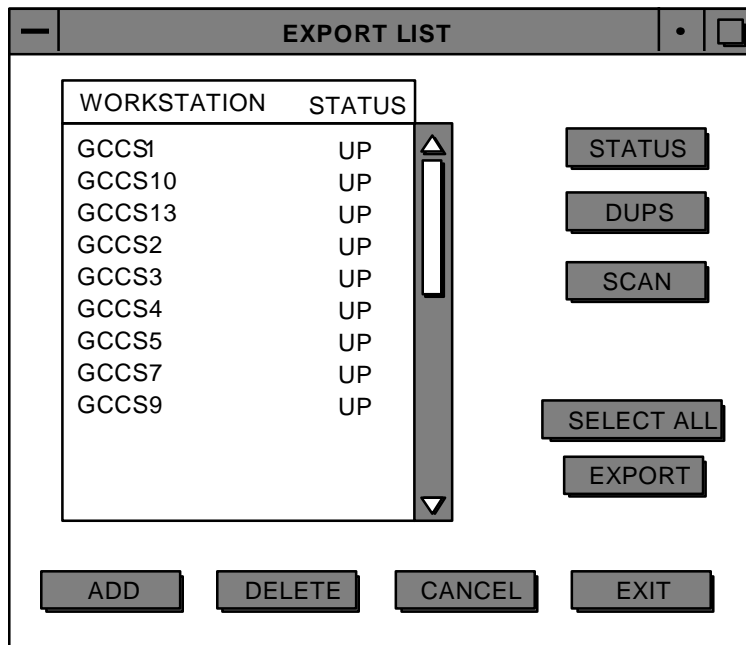
1. Toggle menus and options ON or OFF. (All menus and options are ON when a role is created.)

- If a menu or option is ON (shaded) it is available to a user assigned this role.
  - If a menu or option is OFF (blank) it will not appear on the menubar or the pull-down menu for a user assigned this role.
2. Click OK to accept the changes (or CANCEL to discard)
  3. Repeat this process for other menubars in the scroll list.

## 10.2 EXPORT ROLES

Use this option to maintain user roles on a single workstation and export the updated information to multiple workstations on the LAN.

**To access this window:** ACCOUNTS menu : EXPORT ROLES option : EXPORT LIST window (Figure 10-9).



*Figure 10-9 Export List Window*

The window contains a scroll list of workstations on the LAN. Maintain the workstation list to prepare to export accounts and roles:

- Check the status of all workstations.
- Check for duplicate workstation entries.
- Add or delete workstations.

***How to use the EXPORT LIST Window:***

1. **Warning:** User accounts and roles from the local machine will *overwrite* the user role information on the destination machines.
2. Update role information on this workstation. (See *View Roles*.)
3. Check the status of the destination machines using the STATUS or SCAN buttons.
4. Select the destination machines in the workstation list (or click SELECT ALL).
5. Click EXPORT to send the updated accounts and roles to the selected workstations.

***EXPORT LIST Window Buttons:***

STATUS– pings each workstation in the list.

- A workstation which responds is labeled UP in the status column.
- A workstation which does not respond is labeled DOWN.
- Double-click on a workstation in the list to check its status.
- The STATUS function may be run at any time and does not interfere with the network.

DUPS– checks for multiple workstation entries with the same network and host identification. When duplicates are found, they are listed in the REMOVE DUPLICATES window.

1. Highlight an entry in the REMOVE DUPLICATES window scroll list.
2. Click SELECT to remove that duplicate workstation name.
3. Click SKIP to retain both workstation names and go to the next duplicate.
4. Click ABORT to close the window.

SCAN– searches the network for all available GCCS workstations.

- Displays the total number of workstations added to the list.
- This function can be run at any time and does not interfere with the network.

SELECT ALL– highlights all workstations on the list.

EXPORT– exports role information from the local machine to selected machines.

1. Highlight the destination machines (must be designated as UP).



2. Click EXPORT.

ADD– a workstation to the list.

1. Click ADD to open the ADD W/S window.
2. Enter the new workstation name.
3. Click OK to add it to the list or click CANCEL to discard the change.

DELETE– removes workstations from the list.

1. Highlight the workstations
2. Click DELETE.

CANCEL– discards changes made to the workstation list and closes the window.

EXIT– saves changes to the workstation list and closes the window.

***EXPORT LIST Pop-up Menu Options:***

Pop-up menu options SELECT ALL, ADD, DELETE, STATUS, DUPS, SCAN, EXPORT, CANCEL, and EXIT perform the same as the window buttons. In addition, the following functions are available:

***UNSELECT ALL***

Unselect all workstations in the list.

## **Notes**

## **CHAPTER 11: PRINTING**

Before JMCIS operators have access to printers, two steps must be taken:

1. Define the printers available on the network and identify which workstations have access to each printer. This is a System Administrator function that cannot be accessed by JMCIS operators.
2. On each workstation, identify the default line, graphic, and UNIX printers for that workstation. Use the PRINTER CHOOSER option on the MISC pull-down menu.

This procedure must be followed when JMCIS applications are loaded and whenever printers are added, relocated, or removed from the network.

### ***Printing From a JMCIS Option***

In many windows, a printed report summarizing the window information can be generated using the PRINT function. Choosing PRINT opens the JMCIS PRINTER window (Figure 11-1) to identify where the report will be printed.

**JMCIS PRINTER CHOOSER**

**SELECTED PRINTER**

COPIES: 001                      HOST: jots1  
 PRINTER: HP LASERJET IV        DEVICE: TTYA  
    STATUS: NO ENTRIES

PRINTER NAME	HOST	REMARKS
CANON-BUBBLEJT	jots1	
ALPS	jots1	
HP-PAINTJET	jots1	
HP LASERJET IV	jots1	

**DEFAULT LINE PRINTER**

PRINTER:  
 HOST:  
 DEVICE:

**DEFAULT GRAPHIC PRINTER**

PRINTER:  
 HOST:  
 DEVICE:

*Figure 11-1 JMCIS PRINTER Window*

When the window appears, the printer listed in the **SELECTED PRINTER** box is the default printer, also shown in the **DEFAULT PRINTER** box.

To send the report to the printer:

1. Choose a printer.
  - To use the default printer, no action is required.
  - To choose a different printer, highlight the printer in the scroll list. The fields for this printer appear in the **SELECTED PRINTER** box. Figure 11-1 shows another printer selected.
2. Specify the number of **COPIES** in the **SELECTED PRINTER** box.
3. Click **OK** to send the report to the selected printer, or click **CANCEL** to discard the print request.

### ***JMCIS PRINTER Window Fields***

The window contains two boxes, **SELECTED PRINTER** and **DEFAULT PRINTER**, and a scroll list.

- All fields in the SELECTED PRINTER box *except* COPIES cannot be edited.
- All fields in the DEFAULT PRINTER box cannot be edited. Another default printer is selected using the PRINTER CHOOSER option (MISC pull-down menu).

The fields in the SELECTED PRINTER and DEFAULT PRINTER boxes are:

**PRINTER**

Printer type.

**NAME**

Printer name.

**HOST**

Workstation to which the printer is connected.

**STATUS**

Indicates if the printer is ready or in use.

**COPIES**

Number of copies to print. To change the value in the SELECTED PRINTER box, enter a number. In the DEFAULT PRINTER box this field is view only.

The scroll list displays a list of printers on the LAN available to this workstation. The following columns are displayed for each printer:

**PRINTER NAME**

Printer type.

**HOST**

Workstation to which the printer is connected.

**REMARKS**

Remarks about the printer.

## Notes